2

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

COMPARATIVE ASSESSMENT
OF
U. S. MARINE CORPS
DISASTER RECOVERY PLANS FOR
INFORMATION SYSTEMS

by

Peter J. Hural

September 1992

Thesis Advisor William J. Haga

Approved for public release; distribution is unlimited.

11 Title (Include Security Classification)
Comparative Assessment of U. S. Marine Corps Disaster Recovery Plans for Information Systems

12 Personal Author(s)
Hural, Peter J.

13a Type of Report Master's Thesis	13b Time Covered From To	14 Date of Report (year, month, day) September 1992	15 Page count 68

16 Supplementary Notation
The view expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the US Government.

17 Cost Codes:	Field	Group	Subgroup

18 Subject Terms *(continue on reverse if necessary and identity by block number)*
Disaster, Planning, Recovery

19 Abstract *(continue on reverse if necessary and identity by block number)*

This thesis sets out the basic elements that constitute disaster recovery plans for information systems in DOD based upon a review of private industry plans and DOD requirements. From those elements, a model of a disaster recovery plan is proposed. One of the disaster recovery plans used by the U. S. Marine Corps is presented for comparison to the model plan. A disaster planning checklist to organize and schedule future work in developing a plan and an outline of the U. S. Marine Corps plan are provided. Conclusions are drawn from the comparison and recommendations are put forth for DOD disaster recovery planning to protect information systems.

Comparative Assessment of U. S. Marine Corps Disaster Recovery Plans for Information Systems

by

Peter J. Hural
Major, United States Marine Corps
B.S., Pennsylvania State University, 1978

Submitted in partial fulfillment of the requirements for
the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
September 1992

Author: ______________________
Peter J. Hural

Approved by: ______________________
William J. Haga, Thesis Advisor

____
Roger Stemp, Second Reader

____
David R. Whipple, Chairman
Department of Administrative Sciences

ABSTRACT

This thesis sets out the basic elements that constitute disaster recovery plans for information systems in DOD based upon a review of private industry plans and DOD requirements. From these elements, a model of a disaster recovery plan is proposed. One of the disaster recovery plans used by the U. S. Marine Corps is presented for comparison to the model plan. A disaster planning checklist to organize and schedule future work in developing a plan and an outline of the U. S. Marine Corps plan are provided. Conclusions are drawn from the comparison and recommendations are put forth for DOD disaster recovery planning to protect information systems.

TABLE OF CONTENTS

I. INTRODUCTION

A. PURPOSE

The purpose of this thesis is to identify the risks, possible solutions, and preventive steps that can be taken by information systems managers in the event of a natural disaster. It is not meant to be a guide, but rather, it will attempt to point out ways to recover from a disaster.

A review of the geographical location of military installations reveals that none are immune to the threat of a natural disaster. Natural disasters which have struck various military communities serve as examples to raise our level of awareness concerning the potential threat which these phenomena pose to not only military readiness, but also information systems. In September 1989, Hurricane Hugo tore through the coastal city of Charleston, South Carolina. Military bases that were affected by this hurricane included Marine Corps Air Station Beaufort, South Carolina, and Marine Corps Base Camp Lejeune, North Carolina. In October 1989, the Loma Prieta earthquake rocked North California with the speed and damage that it caused. Military bases that were affected included Naval Air Stations Alameda and Moffett Field. More recently, the Mount Pinatubo volcano eruption in the Philippines caused the abandonment of Clark Air Force Base. Most recently, Hurricane Andrew totally destroyed

Homestead Air Force Base in southern Florida. Natural disasters, although not an everyday occurrence do happen and they are an unavoidable fact of nature.

B. DISCUSSION

Simply stated, disaster recovery planning is an organization's ability to continue its day-to-day operations despite an occurrence of a catastrophic nature, through a series of coordinated and preplanned activities. Successful disaster recovery planning can be achieved with the awareness and endorsement of senior management. In this context, it can be viewed as an informal insurance policy which provides business perpetuity through an attitude that information systems are a critical organizational resource. [Ref. 1]

Disaster recovery planning is an integral part of computer security and, up until a few years ago, was often overlooked or taken for granted. This thesis will attempt to research the area of disaster recovery planning in the civilian and military sectors. Comparisons of the individual plans will be made and effectiveness measured.

The first step in the disaster recovery planning process is deciding that a plan is in fact needed. The damage caused by the Loma Prieta earthquake, Hurricane Hugo, and the Mount Pinatubo volcano eruption serves as a poignant illustration for the necessity of a plan. The plan must identify key personnel and their responsibilities before, during, and after the disaster. Of course, depending on the nature of the disaster, there may be no advance warning, and initially, personal safety may be of the utmost significance.

C. SCOPE

This thesis provides a review and comparison of current U. S. Marine Corps disaster recovery plans to industry plans. No one comprehensive industry plan was available. However, industrial plans were derived from numerous sources on the subject, magazine articles, and seminar and conference outlines. Disaster recovery plans for the Marine Corps were obtained from two Regional Automated Services Centers at Marine Corps Bases Camp Pendleton, California, and Camp Lejeune, North Carolina.

Natural disasters are defined as an occurrence of a catastrophic nature caused by the effects of nature. Examples of natural disasters are: earthquakes, volcanoes, hurricanes, floods, and fires. In addition to natural disasters there are also man-made disasters which require some type of human intervention in order to occur. Examples of man-made disasters are: arson, sabotage, terrorism, computer virus introduction, and sometimes negligence. Prevention is the first step in dealing with man-made occurrences and is normally a security issue. While portions or all of a disaster recovery plan could be implemented for both types of disasters, this thesis will limit its scope to natural disasters.

D. THE REST OF THE THESIS

A review of the literature available on industry disaster recovery is contained in Chapter II. Using this information, a model plan was formulated in Chapter III. Chapter IV contains an overview of current U. S. Marine Corps disaster recovery planning now in use and Chapter V is comprised of conclusions and recommendations. Appendix A is a disaster planning checklist for evaluating current programs and future work and Appendix B contains the outline of the U. S. Regional Automated Services Center disaster recovery plan.

I1. INDUSTRY PLANS FOR DISASTER RECOVERY PLANNING

A. OVERVIEW

Review of industry plans reveals that disaster recovery planning is generally broken down into four main categories or phases. These categories are listed below in their natural order of occurrence:

1. Planning Phase
2. Preparation Phase
3. Implementation Phase
4. Recovery Phase

Each of these phases contain stages or sub-phases. For example, preliminary planning and plan development are sub-stages in the planning phase; while training, drills, and inventory are components of the preparation phase. Work in more than one phase or sub-phase may be accomplished simultaneously.

B. PHASE DESCRIPTIONS

1. Planning Phase: Discussion

Proper planning is essential in both the military and business communities. Terms such as strategic planning and tactical planning are commonly used in both environments. However, a disaster recovery plan for information systems is different in terms of its technical nature and could be a 'hard sell' to management. Most executives or managers would prefer to have a business proposal to decide on rather than a disaster recovery plan. For this reason, convincing management that a plan is indeed needed is the first step in the planning phase and is included in the preliminary planning sub-phase.

a. Preliminary Planning

Proper preparation prior to actually entering the planning phase is crucial since the plan must have management's approval and endorsement, if it is to 'ever get off the ground'. If the disaster recovery plan is viewed as a business plan in terms of monetary loss due to system downtime, then management will be more inclined to lend their support and endorsement. Some of the basic preliminary planning steps include:

- Defining the problem
- Determining the risks involved
- Determining the probability of a disaster occurring
- Determining the impact or loss of services due to an occurrence
- Promoting management support and endorsement
- Planning team composition and assignment of responsibilities

b. Plan Development

Once the preliminary planning phase has been properly completed, the plan can be developed. The plan itself is divided into four phases: the Planning Phase, the Preparation Phase, the Implementation Phase, and the Recovery Phase.

c. Planning Phase

The planning phase of the disaster recovery plan is used to develop the plans, programs, policies, and procedures to be put into operation that will reduce the effects of a natural disaster on an organization's information system. The objective during this developmental phase is to design and implement a set of straightforward policies, programs, and procedures which answer the following questions:

- What is the risk?
- How vulnerable is the organization to that risk?
- What steps will taken prior to the disaster occurrence?
- What steps will taken during the disaster?
- Who will be responsible for these steps?
- What follow-up procedures will be taken?

2. Preparation Phase

The preparation phase will implement the procedures identified by the requirements in the planning phase. It includes actions to be taken in the event that advance notification of an impending disaster is available. It also contains standard procedures to be followed on a daily, weekly, and monthly basis in order to be prepared should a disaster occur without prior or advance notice.

a. Purpose

The specific purpose of the preparation phase is to allow the organization to respond to the impending threat of a disaster. It is in this phase that the plans, policies, and procedures of the planning stage are implemented in a non-emergency environment. The preparation phase includes the following:

- Physical inventory
- Risk assessment
- Alternative technologies
- Environmental conditions
- Training [Ref. 1]

b. Physical Inventory

A comprehensive list of all of the organization's assets by department, application, and service must be compiled. The physical inventory encompasses more than a list of hardware. In essence, everything must be inventoried. Items included in the physical inventory are:

- Internal telecommunications equipment
- Media
- Data communications
- Wiring systems and diagrams
- Physical environment of the facility [Ref. 1]

c. Risk Assessment

Once a comprehensive inventory has been conducted a risk assessment is accomplished. Included in the risk assessment are physical security of the building, carrier hand-off facilities (if used), alternative routes, and specific environmental conditions, including electrical, fire, and water exposures. The basic steps of risk assessment are:

- Identify assets
- Determine vulnerabilities
- Estimate likelihood of exploitation
- Compute expected annual loss
- Survey applicable controls and their cost
- Project annual savings of controls [Ref. 2]

d. Alternative Technologies

Alternative technologies that are available for use are CATV, fiber optics, infrared, microwave, and satellite. An examination into using existing types of existing services should also be performed. There are vendors that provide backup sites for use in the event that your system goes down. A cold site is a facility with power and cooling available, where a computing system can be installed to begin immediate operation. In contrast, a hot site is a computer facility with an installed and ready to run computer system. The system has peripherals, telecommunication lines, power supply, and can come staffed or unstaffed. To activate a hot site, all you do is upload your software and data from off-site backup sites. However, the first step in being able to use this service is a complete and timely backup. Probably the most significant key to successful recovery is backup, which is a copy of all or part of a file to assist in reestablishing a lost file. The concept of backups is divided into three categories. A complete backup is accomplished when everything on the system is copied so the system can be regenerated after a crisis. A revolving backup is one in which the last several backups are kept and each time a backup is done the oldest backup is replaced. In a selective backup only the files that have been changed or created since the last backup are saved. Hand-in-hand with this concept is off-site backup. A backup is useless if it is destroyed in the crisis too. A backup version separate and apart from the system reduces the risk of loss. There are a number of vendors that rent warehouse space for storage of backup data. Finally, in terms of alternatives, vendors and carriers have some plan in place to assist the user with disaster recovery options. [Ref. 2]

e. *Team Identification and Training*

Specific team members are identified along with their responsibilities before, during, and after a disaster. Included in this section should be an outline of the general and specific format for employee training and plan testing.

3. Implementation Phase

The implementation phase of the plan describes the procedures to be followed when it has been determined to initiate the disaster recovery plan. This phase could be put into effect in stages. For example, it may be implemented as a hurricane approaches the organization's location, or it could be activated after a sudden earthquake.

This phase moves the organization from the non-emergency preparation phase into actual activation of the disaster recovery plan. Depending on the amount of advance notice and type of disaster, transition to this phase may be a smooth and natural process. However, if struck by an unforeseen or unforecasted disaster such as a sudden earthquake, the organization may find itself in the recovery phase in very little time.

This phase is the test for the planning and preparation stages. In order to be successful in this stage, the organizations disaster recovery plan must:

- Be easy to read with clear objectives
- Have a thorough index and table of contents
- Be clearly tabbed by appropriate sections

- Have disaster team identification, organization, and responsibilities
- Contain information needed by key personnel to respond to a specific disaster
- Contain specific information that the user would not reasonably be expected to memorize
- Contain enough information so that a backup/alternate user will be able to successfully follow the directions

A document that fits this description and that is in every squadron ready room is the mishap plan. This is a very detailed document with steps to follow in the event of an aircraft mishap. It is a one source document that contains all the procedures to be followed if an airplane were to crash. This, in essence, is what the disaster recovery plan should be - a one source document covering all the procedures to be followed in the event of a disaster.

4. Recovery Phase

This phase of plan development will outline those procedures that will be initiated after the disaster, to bring the organization back to its original operating level. These steps should be initiated as soon as possible.

The purpose of this phase is to restore the organization to normal pre-disaster operation. It begins when the danger to personnel and the effects of the disaster have been neutralized. The amount of damage that the organization has been exposed to determines the level of recovery required. If the damage was minimal, recovery could be as easy as reestablishing power and going back to work.

However, if there is structural damage to the building or if it has been destroyed, then movement to the backup sites will be dictated.

III. DISASTER RECOVERY PLAN MODEL

A. DISCUSSION

Utilizing the four phases outlined in Chapter Two, a sample disaster recovery plan has been formulated. Since all organizations and plans are unique, there is no universal plan that will fit all organizations. This shell may suit a certain type of organization well, but for others, some modifications may be necessary. The model plan below is intended to illustrate the policies to be adhered to, the points to be covered, and the actions to be taken in the event of a natural disaster.

B. PLANNING PHASE: PLAN DEVELOPMENT

The disaster recovery plan should begin with a policy statement stating its purpose and objectives. The main issues to be covered are described below.

1. Purpose

To establish an organization-wide disaster recovery that will protect and minimize the damage or loss incurred by the organization. This will include:

- Definition and scope of the plan
- Determination of risk to the organization
- A business impact analysis
- Prevention strategies
- Revision and update procedures

- Departments affected
- Reference documents
- Responsibilities
- Definition of recovery strategies [Ref. 1]

2. Objectives

To state what the plan is attempting to accomplish. The plan must be consistent with organizational strategy.

- Protect human life
- Minimize loss and risk to the organization
- Maximize recovery and return to normal operations [Ref.1]

C. PREPARATION PHASE

This section will deal with policies and procedures to be utilized in a non-emergency environment in preparation for a forecasted disaster. This phase also includes normal everyday procedures to be adhered to in order to lessen the impact of an unforecasted disaster. Training and drills are also included in this phase.

1. Policies

A statement of policy regarding daily business guidelines to be practiced, and non-emergency procedures to be followed in the event of an impending disaster. A policy statement on the formulation of a training plan is also included.

- Purpose
- Scope
- Definitions and responsibilities

- Departments affected
- Reference documents [Ref. 1]

2. Procedures

A list of the procedures to be adhered to during daily operations, and to ensure a smooth and orderly transition into the implementation and recovery phases. The procedures for following the training plan, and the frequency of drills will all be covered.

- Backup procedures
- Off site storage procedures
- Notify disaster teams
- Notify all levels of management
- Inform employees
- Frequency of training
- Conduct of drills
- Evaluate results
- New employees [Ref. 1]

D. IMPLEMENTATION AND RECOVERY PHASE

1. Policy

These phases would typically be activated after the disaster has occurred and outline the responsibilities of the disaster teams, critical applications, and personnel involved.

- Scope of the organizations' involvement
- Affected departments and personnel
- References to other policies and company standards

- Definition of responsibilities
- Job descriptions for teams/members [Ref. 1]

2. Procedures

This section will describe actual actions taken after event detection. It will cover various types of emergencies or events that have been outlined in the plan.

A. Event detection/recognition

B. Types of events or emergencies

- Hardware failure
- Software failure
- Telecommunications failure
- Fire
- Flood
- Earthquake
- Hurricane
- Cable cut
- Power loss
- Other as needed

C. Damage assessment

D. Action to be taken

- Protect human life
- Notify fire, police, medical, management
- Determine nature and cause of disaster
- Minimize the effects of the disaster
- Inform vendors, employees

E. Recovery/operations resumption

- Activate disaster teams
- Activate backup procedures
- Relocate to hot site (if applicable)
- Reroute network facilities
- Re-establish connectivity and facilities
- Track work for audit purposes
- Maintain systems and facilities security
- Begin the cleanup effort

F. Migration and restoration procedures

- Reconstruct site
- Restore hardware systems
- Restore software systems
- Restore uninterruptable power supply
- Replace detection and suppression systems
- Secure the area
- Rewire facility
- Train/retrain employees on new equipment
- Clean up area
- Schedule migration back to site
- Keep management and employees informed
- Coordinate return to normalcy

3. Appendices

This section of the plan should contain a detailed list of the appendices used. They should be indexed and cross-referenced, and maintained to be as current as possible. Some suggested appendices are:

- Disaster team composition
- Emergency call lists for teams, managers, and authorities
- Inventory and report forms
- Application lists
- Hardware lists
- Software lists
- Vendor call lists
- Contract and maintenance agreements
- Test forms [Ref. 1]

IV. OVERVIEW OF U. S. MARINE CORPS DISASTER PLANNING

A. DISCUSSION

The disaster recovery plans that were reviewed were obtained from the Regional Automated Services Centers at Marine Corps Bases Camp Lejeune, North Carolina, and Camp Pendleton, California. The Regional Automated Services Centers are responsible for administrative data processing for their respective East and West coasts. For example, the Regional Automated Services Center at Camp Pendleton provides support for Marine Corps Air Station, Yuma, Arizona, four Marine Corps Bases and Air Stations in California, and those located in Hawaii. The data processed by the Regional Automated Services Center include logistics, finance, aviation, and manpower. It also runs the Marine Corps Data Network for the West Coast in addition to operating a local area network. The Regional Automated Services Center is comprised of the following branches:

- Executive Branch
- Applications Program Branch
- Technical Support Branch
- Processing Branch

The Executive Branch is responsible for administrative functions, supply, budget, security, and training. The

Applications Program Branch is accountable for program development and maintenance. The Technical Support Branch is composed of an Operating System Section, Teleprocessing Section, and a Database Section, each with their respective duties and responsibilities. The Processing Branch is responsible for the day to day operations of the Center. The title of the disaster recovery plan in use is the Transportable Contingency Action Plan. This chapter will summarize the content of the plan.

B. OVERVIEW

The Transportable Contingency Action Plan is broken down into the following parts or phases:

1. Preliminary Planning
2. Preparatory Actions
3. Action Plan
4. Enclosures/Appendices

A more detailed examination of these phases and their components follows in the sections below.

C. PRELIMINARY PLANNING

The preliminary planning phase is comprised of the following sections:

1. Record of Changes
2. Introduction
3. Objectives and Scope
4. Assumptions

5. Responsibilities

6. Strategy

1. Record of Changes

This section provides an update and revision mechanism for the contingency plan and includes monthly and annual reviews.

2. Introduction

The contingency plan introduces the elements of emergency response, backup operations, and recovery procedures. Emergency response is described as those procedures to cover the appropriate response to defined disasters, backup operations describe the procedures for movement to a backup site, and recovery procedures cover those tasks following physical destruction or major damage and loss of data.

3. Objectives and Scope

This section contains statements on the purpose, scope, and objectives of the contingency plan. The stated purpose of the plan is to reduce the consequences of loss of computer resources or capabilities to an acceptable level. The objectives and scope are to minimize the turbulence caused by unexpected loss of data processing support and to test the plan annually.

4. Assumptions

The contingency plan makes assumptions about which events to include or exclude. Included events are fire, natural disaster, power instability, or environmental control failure. Those events that are excluded are software errors, data entry problems and misuse of hardware. The contingency plan is based on a set of priorities given in a risk assessment that is performed annually. There is also a delineation of support responsibilities should the Regional Automated Service Center need it.

5. Responsibilities

This section of the plan outlines the responsibilities for plan preparation and maintenance and contains the procedures to be followed by the individual departments of the center, and includes an emergency chain of command.

6. Strategy

The plan is designed to restore processing at a designated backup site in the event of a disaster. A disaster is defined as any event that makes the center unable to provide mainframe production support for a period exceeding 10 days. It includes procedures for emergency response and contains a disaster classification. A Level I disaster is defined as partial destruction of the tape library or critical equipment that would require on-site processing with backup equipment at reduced efficiency. A Level II disaster is a major equipment malfunction that would exceed 10 days down time, and a Level III disaster is total destruction of the installation requiring movement to the backup site.

Included in this section are policies and procedures for disaster prevention, these include: backup and recovery, emergency generator, power conditioning equipment, uninterruptable power supply system, fire and evacuation plan, recall roster, security measures, and disaster team responsibilities.

D. PREPARATORY ACTIONS

The preparatory actions phase is comprised of the following sections:

1. Personnel
2. Data
3. Application Software
4. Hardware and System Software
5. Communications
6. Supplies
7. Transportation
8. Space
9. Power and Equipment
10. Documentation
11. Test Plans

1. Personnel

This section contains disaster recovery team composition and assignment, recall rosters, and emergency notification rosters.

2. Data

This section contains the policies and procedures regarding weekly and incremental backup and off-site storage and a listing of critical data files required for backup site processing.

3. Application Software

Application software is included in the full system backup which are created weekly and stored at the off-site storage facility.

4. Hardware and System Software

This section deals with the hardware requirements at the backup site and backup schedules for systems and production software.

5. Communications

This section provides both the current on-site communications requirements and the back-up site requirements.

6. Supplies

Lists of necessary office supplies, critical supply items, and vendors who provide supplies are contained in this section.

7. Transportation

The transportation section contains the procedures for coordination of transportation needs/arrangements to the backup site including commercial air, and military transport.

8. **Space**

The space for the system at the current site and backup site are outlined in this section.

9. **Power and Equipment**

This section provides the power and environmental requirements for the current site and the backup site.

10. **Documentation**

All of the required information for system restoration and operations is contained in the contingency plan and enclosures.

11. **Test Plans**

The test plans section sets the policies and procedures for annual testing, requisite personnel, schedule of events, and evaluation procedures.

E. ACTION PLAN

The Action Plan gives personnel procedures to follow in a variety of emergency occurrences that may happen and is comprised of the following sections:

1. Emergency Response
2. Backup Operations
3. Recovery Operations

1. **Emergency Response**

This section outlines the emergency response procedures to be followed in the event of a power outage, air-conditioning failure, fire, down machinery, lost software, bomb threat, and destruction to the building.

2. Backup Operations

This section describes the procedures to be followed for backup operations in the various disaster scenarios listed above.

3. Recovery Operations

This section contains the procedures to transfer processing to backup site and prepare necessary software and data to be taken, in the various scenarios listed above.

F. ENCLOSURES

The following is a list of enclosures that are contained in the Transportable Contingency Action Plan:

- Contingency Plan Checklist
- Off-site Storage
- Regional Automated Services Center Standard Operating Procedures
- Operations Standard Operating Procedures Extract
- Recall Roster
- Processing Support Section Standard Operating Procedures Extract
- Processing Contingency Plan
- Operational Support Airlift Management
- Systems Contingency Standard Operating Procedures
- Telecommunication Contingency Standard Operating Procedures
- Database Contingency Standard Operating Procedures
- Emergency Notification Roster
- Disaster Recovery Teams

- Critical Data Files
- Critical Supplies - Vendor Addresses
- RASC Computer Room (App. B)

V. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

This thesis stresses the significance of a disaster recovery planning strategy to lessen the impact of a natural disaster on an informations systems organization. The importance of disaster recovery planning cannot be overstressed. Planning for a disaster sets up a rational process and establishes decision making criteria. As a process, planning for a disaster forces management to look ahead at the inevitability of a disaster occurring. It requires communications within the organization about goals, strategic issues, and resource allocation in preparing for and responding to a natural disaster. It stimulates longer term analyses than would otherwise be made, creating a proactive environment instead of a reactive one. Finally, by using a planned strategy to deal with a natural disaster, the command/organization sets priorities, policies, and procedures to control an unfamiliar and chaotic event.

The Transportable Contingency Action Plans in use by the Regional Automated Services Centers illustrate these points. The plan is comprehensive, well thought out, and detailed. It is put to the proof annually allowing two days of testing and evaluation. A significant feature of these plans is the existence of a reciprocal backup agreement between the two centers. If the West Coast Center goes down, the East Coast Center is the backup site, and vice versa. Their plan is reviewed monthly and again on an annual basis, allowing for the most current updates and revisions. Additionally, both of the Regional Automated Service Centers keep each other informed of the latest innovations and technologies for disaster recovery plan maintenance.

B. RECOMMENDATIONS

The occurrence of natural disasters will continue to plague us. Some of the most recent incidents that directly affected military installations are the Mount Pinatubo volcano eruption in the Philippines, Hurricane Andrew in southern Florida, and Hurricane Iniki in Hawaii. An evaluation of the disaster recovery plans in use by the military installations that were touched by these disasters and how well they worked, offer a number of theses topics. The procedures utilized by information systems personnel at these locations should be examined to provide the most updated information on the effectiveness of military disaster recovery planning and the results of the efforts in the aftermath.

APPENDIX A

DISASTER PLANNING CHECKLIST

This disaster planning checklist is provided as an aid to identify an organization's present situation and to organize and schedule future tasks in developing a sound disaster recovery plan. It is broken down into major categories that are applicable to almost all information systems organizations. This checklist is designed to be a working paper that can be updated as events occur. [Ref. 3]

GENERAL OVERVIEW

	YES	NO	WIP	ASSIGN / ACTION
1. If a major disaster to your data center occurred today, could your organization survive?				
2. Have you recently completed an Impact/ Risk Analysis?				
3. Do you know the total dollar amount of your exposure?				
4. Have you prioritized all of your programs?				
5. Have you listed the maximum downtime for all of your systems?				
6. Have you listed the objectives of a disaster plan and the assumptions it includes?				
7. Do you have a disaster plan, and is it current?				
8. Does the Plan include backup facilities?				
Hot backup site?				
Cold site?				
Reciprocal agreement?				
9. Does the backup facility inform you when there is a change in hardware or software?				
10. Have you determined the cost of a disaster plan including:				
Initial cost?				
Development cost?				
Maintenance cost?				
11. Has the plan been approved by top management?				
12. Do you have a Disaster Planning Coordinator?				
13. Is someone assigned to update the plan?				
14. Does the plan use a team approach?				
15. Do you have people assigned to lead each team?				
16. Is the same person assigned to lead more than one team?				
17. Are names and phone numbers updated regularly?				

Disaster Recovery Plan

	YES	NO	WIP	ASSIGN / ACTION
18. Has the plan been reviewed by the Internal Audit, Security, and Insurance Departments?				
19. Does the plan provide for recovery from a major disaster, and can it be adjusted for a less severe occurance?				
20. Has the plan been tested using only material stored off-site?				
21. Is the plan tested at least every 6 months?				
22. Has the plan been updated as a result of the testing?				
23. Have you ever initiated a surprise test?				
24. Does the plan provide instructions for:				
Emergency procedures?				
Organizational structure following a disaster?				
Off-site storage for all recovery material?				
25. Does the off-site storage have 24-hour access, physical security, vaulting, fire protection, courier service, round trip travel time of less than 1 hour, access only by authorized persons?				
26. Are the tapes secured in a separately controlled room within the secured area?				
27. Is all system documentation, except program listings, kept in fireproof storage when not in use?				
28. Are there written instructions that define the responsibilities that personal computer (PC) users have for backing up and protecting their files?				
29. Have these instructions been given to all PC users?				
30. Have all data center personnel been advised about the confidentiality of all information they work with?				

DATA CENTER FACILITY

	YES	NO	WIP	ASSIGN / ACTION
1. Are there signs outside identifying the data center?				
2. Is the building protected by security guards, fences, alarm systems, and/or closed-circuit monitoring?				
3. Is wiring for all security and alarm systems passed through conduit?				
4. Do the guards make scheduled rounds of the building?				
5. If no guards are used, are the people responsible for security trained by security professionals?				
6. Has someone been assigned the responsibility for security of the data center, company, or building?				
7. Are security personnel or computer room personnel on site at all times?				
8. Is there card access to the facility and various areas in the facility?				
9. Are identification badges worn by all employees?				
10. Are visitors required to sign in and sign out?				
11. Is there security at the receiving area?				
12. Is there an Office/Building Emergency Booklet published that includes:				
Medical emergencies?				
Fire emergency procedures?				
Evacuation procedures?				
Bomb threats?				
Security violations?				
Electrical failures?				
13. Has someone been assigned to provide information, instruction, and supervision for the list in Item 12?				
14. Are evacuation route drawings posted in all hallways?				
15. Have all occupants been instructed and trained in emergency procedures?				

Disaster Recovery Plan

	YES	NO	WIP	ASSIGN / ACTION
16. Are fire drills conducted on a regular basis under the supervision of your local fire marshall?				
17. Is there a written termination procedure that includes a checklist of items to be returned to the company, such as keys, ID badges, card access, etc.?				
18. Are all employees required to take vacation time so others can perform their duties?				
19. Do all areas of all buildings have a fire alarm system?				
20. Has the fire detection and extinguishing equipment been tested and/or inspected in the past 6 months?				
21. Does the insurance company or fire department make annual fire inspections?				
22. Is the storage area for forms and supplies protected with sprinklers?				
23. Are smoke detectors located in the storage area?				

DATA ENTRY

	YES	NO	WIP	ASSIGN / ACTION
1. Are there alternatives for entering input normally keyed on-line?				
2. Have you made provisions to have keying done on the outside in emergencies?				
3. Is a copy of the keying instructions stored off site?				
4. Is a software package used for keying, and is it available to outside services?				
5. Have arrangements been made to have your affiliates or divisions key your input?				
6. Are all manual procedures performed by data entry documented and a copy stored off site?				
7. Are source documents batched and controlled by another department?				
8. Are source documents stamped with date, time, and operator after keying?				
9. Are source documents maintained in their original batches for a short time so they can be rekeyed if necessary?				
10. Are source documents returned to the data control department after keying?				
11. Can the data entry department be reestablished in another location in a reasonably short time if necessary?				

DATA CONTROL

	YES	NO	WIP	ASSIGN / ACTION
1. Is access to the data control department restricted?				
2. Are all source documents and computer reports routed through this department for control and balancing?				
3. If communication fails for transmitted reports, has an alternate method for sending reports to users been established?				
4. Is this department responsible for the control of check forms?				
5. Is there a written procedure for issuing a supply of blank checks outside the computer room?				
6. Are checks signed by a different person from the person balancing and distributing them?				
7. Can the check signer be replaced overnight?				
8. Is there any special office equipment critical to the operation of the data center, that provisions for a substitute have not been made?				
9. Are backup signature facsimiles secured off site?				
10. Is there a formal custom-form system that identifies all forms, their reorder point, their supplier, and an alternate supplier?				
11. Is a small supply of all critical custom forms maintained off site?				
12. Is a copy of all form specifications and a copy of the final proof maintained off site?				
13. Is a fact sheet maintained on all suppliers of office equipment and forms?				
14. Has an alternate point-to-point pickup and delivery been planned for if the primary method is not operational?				
15. Is there an output distribution report form for every printed report defining: number of copies, decollate, burst, method of shipping, recipient name, and recipient phone number?				

COMPUTER ROOM

	YES	NO	WIP	ASSIGN / ACTION
1. Is access to the computer room restricted?				
2. Are only the computer operators allowed to operate the computer?				
3. Is the room protected by Halon, CO_2, or sprinklers?				
4. Are smoke detectors located:				
In the ceiling?				
Under the raised floor?				
In the air conditioning ducts?				
5. Will the smoke detectors operate even if there is a power outage?				
6. Are fire extinguishers located at all exit doors?				
7. Are water detectors located under the floor?				
8. Are waterproof covers stored in the computer room for emergencies?				
9. Is a UPS system installed for short power outages?				
10. Is a generator available for extended power outages?				
11. Is there emergency lighting in the computer room?				
12. Is there an emergency Power-Off switch located at the exits?				
13. Is there more than one cooling system that will support the computer hardware should one system fail?				
14. Will an alarm sound if the air conditioning system is turned off?				
15. Is the temperature and humidity monitored?				
16. Will some type of visible or audible alarm sound if the limits are exceeded?				
17. Are fire doors installed at all entrances to the computer room?				
18. Are check forms stored in a secured room?				

Disaster Recovery Plan

	YES	NO	WIP	ASSIGN / ACTION
19. Are there written instructions for powering up and powering down the system?				
20. Are there written instructions for actions to take in an emergency?				
21. Is there a copy of the MIS Contingency Plan in the computer room?				
22. Is a procedure library used that contains all the job control necessary to execute job streams?				
23. Is there a formal scheduling system, either computerized or manual?				
24. Is someone assigned to review the schedule and enter all control record information?				
25. Is the entering of control records and similar job control functions eliminated from operator intervention?				
26. Are tape mounts controlled by a tape-librarian system?				
27. Does a supervisor review reasons why an operator overrides the tape-librarian system?				
28. Does operations management review the console log and error listing to ensure that identifiable errors are corrected and recurring errors are prevented?				
29. Are there written restart procedures for all production systems?				
30. Do the restart procedures indicate that other systems may have to be reprocessed even though they completed successfully?				
31. Do all high priority systems have detail recovery procedures documented?				
32. Are all problems in the computer room documented?				
33. Are metered hours correlated to lapsed time if practical?				
34. Is there a formal Problem Management system, where computer room problems are reviewed by members from operations and programming and remedies assigned?				

Computer Room

	YES	NO	WIP	ASSIGN / ACTION
35. Is all down time reviewed by operations management?				
36. Is all production job control reviewed by the operations department after testing is completed and before programs are turned over for production?				
37. Are there Run Manuals for all production applications?				
38. Do the operators have easy access to the Run Manuals?				
39. Are duplicate copies of the Run Manuals stored off site?				
40. Is all special processing for quarterly or annual runs properly documented?				
41. Are batch jobs scheduled for each shift?				
42. Is there a computerized job-accounting system?				
43. Is the job-accounting report reviewed to determine any unusual run patterns?				
44. Are all new systems reviewed for proper file rotation to off-site storage?				
45. Is there a list of all computer hardware including serial numbers, communication equipment and lines, power requirements, cooling requirements, floor space requirements, and acceptable substitute equipment for all the above; and is a copy of this list stored off-site?				
46. Is there a cable layout diagram and plug connector description for the current equipment, and is a copy stored off site?				
47. Is a Vendor Information sheet maintained for all vendors supplying computer equipment and supplies?				
48. Have you asked a used hardware vendor for a list of available equipment, in preparation for an emergency?				
49. Are the following backed up daily and rotated off site:				
Procedure library?				
Tape librarian?				
Job scheduling?				

Disaster Recovery Plan

	YES	NO	WIP	ASSIGN / ACTION
50. Is there a formal procedure for obsoleting a program?				
51. Are the microfiche procedures documented and a copy stored off-site?				
52. Are there any water pipes near or above the computer room?				
53. Is there a threat of water leakage from nearby areas: kitchen, restrooms, janitor closet, drinking fountain?				

TAPE LIBRARY

	YES	NO	WIP	ASSIGN / ACTION
1. Is the tape library protected by Halon, CO_2, or sprinklers?				
2. Are smoke detectors located in the tape library?				
3. Does the entrance to the tape library have a fire door?				
4. Does the tape library have emergency lights?				
5. Is access to the tape library restricted by card access or other security?				
6. Is a fire extinguisher mounted outside the door to the tape library?				
7. Has the tape library become a storage area for items other than tapes?				
8. Does the off-site storage for tapes have security, fire protection, 24-hour access, bonded pickup and delivery?				

TELECOMMUNICATIONS

	YES	NO	WIP	ASSIGN / ACTION
1. Is there a layout of your communications network and is a copy stored off site?				
2. Are the following items part of the layout:				
Number of lines?				
Type of lines?				
Distance of lines?				
Branches off the main line?				
Location of modems by manufacturer, model, and serial number?				
Location and identification of terminals?				
3. Are there written procedures covering failures in the:				
Telecommunication lines?				
Modems?				
Terminals?				
4. Are the lines interchangeable if one of them fails?				
5. Does it take manual intervention to switch the lines?				
6. Is the telecommunications system critical enough to justify the cost of multiple processors?				
7. Are satellites part of the communication system?				
8. Are the satellites protected with the same type of high security as the computer facility?				
9. Is satellite repair/replacement equipment readily available and service on 24-hour call?				
10. Are all on-line transactions identified by date, time, operator, and terminal?				
11. Are passwords required as part of the sign-on procedure?				
12. Is there some alert indication when a user fails the sign-on procedure more than 3 times?				
13. Is an audit trail produced daily that identifies all on-line users?				

Disaster Recovery Plan

	YES	NO	WIP	ASSIGN / ACTION
14. Are passwords routinely changed?				
15. Is someone responsible for updating the password list following a termination?				
16. Is the updating of master files restricted to certain operators or terminals?				
17. Are all terminals locked when they are not in use?				
18. Is cryptography used for sensitive information?				
19. Is sensitive information sent on either leased or dedicated lines?				
20. If dial-up lines are used, is there an automatic callback that completes the connection to the network?				
21. Can the communication network be directed to the hardware at the hot backup site?				
22. Does the on-line system update a large critical database?				
23. Is logging used for the on-line systems?				
24. Do on-line systems have proper recovery for the users if the system goes down?				
25. Are written terminal recovery procedures located at all terminal locations?				
26. Are the recovery procedures routinely tested?				
27. Is input maintained at the terminal location until its acceptance is assured?				
28. Can the input be recreated if it is lost?				
29. Has on-line input been prioritized allowing only critical input to be entered following a disaster?				
30. Can on-line input be forwarded to the data center by alternate methods?				
31. Are workable communications to your network available at the backup facility?				
32. Has the backup facility communications been tested?				

SYSTEMS AND PROGRAMMING

	YES	NO	WIP	ASSIGN / ACTION
1. Is all application software backed up and stored off site?				
2. Do all changes to programs need authorization?				
3. Are there audit trails that identify any program that has been copied for modification, or new program in development?				
4. Is all application software responsible for distributing funds, such as payroll and accounts payable, password protected?				
5. Do the systems above have adequate controls, such as batch totals, hash totals, run totals, and dollar amounts?				
6. Are checks outside the normal range flagged on an audit trail report?				
7. Does an accounts payable audit trail report list the payee for all checks?				
8. Do all financial applications have complete audit trail reports?				
9. Is all of the on-site system documentation stored in fireproof cabinets?				
10. Are users asked to assist in the preparation of test data?				
11. Is there a formal methodology for design and programming?				
12. Is the design phase completed before the programming phase begins?				
13. Are there written design standards and programming standards?				
14. Are all permanent files categorized as critical, important, useful, and non-essential?				
15. Do the standards require the backing up of all critical files?				
16. Are the 3 most current generations of all important and critical files maintained (current, father, grandfather)?				
17. Do the standards require all programs to include proper controls and totals for complete auditing, and for the detection and correction of errors?				

Disaster Recovery Plan

	YES	NO	WIP	ASSIGN / ACTION
18. Is test data with predetermined results saved and used for heavily maintained systems such as payroll?				
19. Are program changes always made to the source code?				
20. Is the source code maintained on a library that is backed up and rotated off site?				
21. Are the program linkedit reports reviewed for errors and filed with the source code listing?				
22. Are programs always tested even when they have minor modifications?				
23. Does management randomly review program changes and test results?				
24. Do user departments sign off on program modifications and review test results?				
25. Is there a formal procedure for making a program in development a production program?				
26. Are operation Run Manuals required as part of the program turnover to operations?				
27. Are all modifications to purchased software fully documented and coded in a way that will not disturb the pure supplied code?				
28. Is a list available of all systems with the person responsible noted?				
29. Is there a list that identifies all programs in a system?				
30. Does each system have a back-up person?				
31. Is documentation kept current?				
32. Is documentation maintained on the computer, backed up, and rotated off site?				
33. Is there a listing of all technical manuals so they can be replaced if necessary?				
34. Does your company policy state the file retention period for corporation assets information, stockholder information, tax records, employee information, and other vital records?				

Computer Room

	YES	NO	WIP	ASSIGN / ACTION
35. Are record layouts maintained for the retention period along with the file media?				
36. Has the source information been identified that created the retained data?				

TECHNICAL SUPPORT

	YES	NO	WIP	ASSIGN / ACTION
1. Is the operating system backed up and rotated off site?				
2. Is a list maintained of all operating system software?				
3. Are the people in the department cross-trained so that everyone has backup?				
4. Are all responsibilities, duties, and procedures documented and a copy stored off site?				
5. Is a Vendor Information sheet maintained for all vendors supplying software?				
6. Have provisions been made for purchased software to execute on another system during an emergency?				
7. Is a copy of the SYSGEN parameters stored off site?				
8. Is there complete documentation explaining how to bring up the operating system at the backup facility?				
9. Is the utilization of all disk devices documented?				
10. Has a plan been formulated on how alternate disk devices would be utilized?				
11. Is there documentation explaining how to modify the JCL to execute at the backup facility?				

DATABASE ADMINISTRATION

	YES	NO	WIP	ASSIGN / ACTION
1. Are all databases identified?				
2. Are all programs that update each database identified?				
3. Is the activity that updates the database continually logged?				
4. Are all programs that access each database identified?				
5. Are databases backed up and rotated off site?				
6. Are audit trails available that identify databases that are filling up, and are these reports available on a daily basis?				
7. Are there documented procedures on how to test the validity of each database after it is restored?				
8. Is there documentation that identifies multiple databases that must be kept synchronized with each other?				

INTERNAL AUDIT

	YES	NO	WIP	ASSIGN / ACTION
1. Have you reviewed the MIS Contingency Plan?				
2. Have you observed a recovery test that only used material stored off site?				
3. Do you periodically review the data center operation and make written recommendations on improvements to procedures, security, and controls?				
4. Are user departments required to balance computer output to manual control totals for audit and security?				
5. Do you save test data to process through cash disbursement systems producing predetermined results?				

INSURANCE

	YES	NO	WIP	ASSIGN / ACTION
1. Has the data center management been informed as to the do's and don'ts concerning insurance following a disastrous event?				
2. Does the insurance policy include business interruption coverage?				
3. Is another department in the organization responsible for insurance protection?				
4. Do you have a copy of the insurance policy?				
5. Have you reviewed the coverage in the past year?				
6. Do you have an annual formal review of your insurance coverage with the insurance carrier?				
7. Does the insurance coverage include data processing hardware and software?				
8. Did you perform a risk/impact analysis for the data center?				

BACKUP FACILITY

	YES	NO	WIP	ASSIGN / ACTION
1. Do you currently subscribe to a fully-equipped backup facility?				
2. Is the backup facility located at a distance that will ensure that an area-wide disaster will not affect the facility?				
3. Is the security at the backup facility at least as good as the security at your current facility?				
4. Have you ever used the backup facility as part of a mock disaster?				
5. Does the backup facility have adequate hours available for testing?				

RECIPROCAL AGREEMENTS

	YES	NO	WIP	ASSIGN / ACTION
1. Do you have a formal reciprocal agreement currently in effect?				
2. Does the other organization's computer have time available to share with you?				
3. Does your computer have time available to share with another organization?				
4. Are both computer systems compatible?				
5. Do both computer systems have the capacity to process critical applications for both organizations at the same time?				
6. Is the operating system software compatible?				
7. Is there sufficient tape and disk capacity and compatibility?				
8. Will your communication network quickly connect with the other organization's computer?				
9. Does either data center have specialized hardware such as laser printers or cartridge tape drives?				
10. Have both organizations agreed to notify the other about changes in hardware or software?				
11. Will your purchased software execute at the other data center?				
12. Have you tested a critical application at the other data center?				
13. Is there temporary storage available at the other data center for printer forms?				
14. Is there temporary storage available at the other data center for your tape library?				
15. Is there temporary office space available at the other data center for operations support personnel?				

APPENDIX B

U. S. MARINE CORPS DISASTER RECOVERY PLAN

The plan outline provided in this appendix is the Transportable Contingency Action Plan currently in use at the Regional Automated Services Center at Camp Pendleton, California. It is provided to illustrate an example of the level of detail necessary in disaster recovery planning.

TABLE OF CONTENTS

1.6.3 Recovery

1.6.3.1 Recovery While Maintaining Processing On-site

1.6.3.2 Processing at Backup Site

1.6.4 System Restoration

1.6.4.1 Disaster Recovery Team

1.6.4.2 Processing/Operations Team

1.6.4.3 Systems Team

1.6.4.4 Acquisition/Administrative Team

SECTION 2. PREPARATORY ACTIONS

2.1 Personnel

2.1.1 Recall Roster

2.1.2 Emergency Notification Roster

2.1.3 Team Composition

2.2 Data

2.2.1 Critical Files Needed For Backup Site Processing

2.3 Application Software

2.4 Hardware and System Software

2.5 Communications

2.5.1 Current On-site Requirements

2.5.2 Requirements for Backup Site(s)

2.6 Supplies

2.6.1 List of Critical Supply Items

2.6.2 List of Vendors Who Provide Supplies

2.6.3 List/Location of Supplies Needed For Backup Site(s)

2.7 Transportation

2.7.1 Requirements For Recovery Operations/Backup Site

2.8 Space

2.8.1 Current Site Requirements

2.8.2 Backup Site Space Available

2.9 Power and Equipment

2.9.1 Current Site Requirements

2.9.2 Backup Site Requirements

2.10 Documentation

2.11 Test Plans

SECTION 3. ACTION PLAN

3.1 Emergency Response

3.1.1 Scenario 1. Power Outage

3.1.2 Scenario 2. Air-conditioning Failure

3.1.3 Scenario 3. Fire

3.1.4 Scenario 4. Down Machinery

3.1.5 Scenario 5. Lost Software

3.1.6 Scenario 6. Bomb Threat

3.1.7 Scenario 7. Building Destroyed

3.2 Backup Operations

3.2.1 Scenario 1. Power Outage

3.2.2 Scenario 2. Air-conditioning Failure

3.2.3 Scenario 3. Fire

3.2.4 Scenario 4. Down Machinery

3.2.5 Scenario 5. Lost Software

3.2.6 Scenario 6 Bomb Threat

ENCLOSURES

LIST OF REFERENCES

1. Bates, R. J., *Disaster Recovery Planning*, pp.6,129-134, McGraw-Hill, Inc.,1992.

2. Pfleeger, C. P., *Security in Computing*, pp. 442-444, 458, Prentice-Hall, 1989.

3. Arnold, R., *Disaster Recovery Plan*, QED Information Sciences, Inc., 1990.

BIBLIOGRAPHY

1. Arnell, A., *Handbook of Effective Disaster/Recovery Planning A Seminar/Workshop Approach*, McGraw-Hill, Inc., 1992.

2. Chantico Series, *Disaster Recovery, Contingency Planning and Program Evaluation*, QED Information Sciences, Inc., 1990.

4. Computer Security Institute, *Disaster Recovery Alternatives in a LAN Environment*, Computer Security Institute, 1992.

5. Computer Security Institute, *Closing the Recovery Window* Computer Security Institute, 1992.

6. IBM Management Institute, *Disaster Recovery Planning,* IBM Management Institute, 1991.

7. Russell, D., and G. T. Gangemi, *Computer Security Basics*, O'Reilly & Associates, Inc., 1991.

9. Wrobel,L. A., *Disaster Recovery Planning for Telecommunications*, Artech House, Inc., 1990.

INITIAL DISTRIBUTION LIST

1. Commandant of the Marine Corps 2
Code TE 06
Headquarters, United States Marine Corps
Washington, D. C. 20380-0001

2. Defense Technical Information Center 2
Cameron Station
Alexandria, Virginia 22304-6145

3. Captain Hammond 1
Regional Automated Services Center
Marine Corps Base
Camp Pendleton, California 92055-5100

4. CWO2 D. L. Kennedy 1
Regional Automated Services Center
Marine Corps Base
Camp Lejeune, North Carolina 28542-5001

5. Dudley Knox Library 2
Code 52
Naval Postgraduate School
Monterey, California 93943-5002

6. Commander 1
Naval Computer and Telecommunications Command
4401 Massachusetts Ave.,N.W.
Washington, D. C. 20394-5000

7. CDR Debbie Campbell 1
National Computer Security Center NSA/C81/APSXI
9800 Savage Road
Ft. Meade, MD 20755-6000

8. Naval Information Systems Management System 1
Bldg. 166
Washington, D. C. 20374-5070

9. SPAWAR 1
Code 2241
Crystal City 5CPK, 700
Washington, D. C. 20363-5100